ARIZONA TRANSPORTATION RESEARCH CENTER

RESEARCH NOTES:

Project 502(1)

February 2001

ADOT USES FOR VIRTUAL PRIVATE NETWORKING TECHNOLOGY: PHASE 1 – PRE-PILOT TEST REPORT

Highlights

- This phase of the project includes the feasibility study for the use of Virtual Private Network technology by ADOT, and especially by the Motor Vehicles Division (MVD) of ADOT.
- Following the feasibility study period, preliminary analysis was conducted to determine potential users of VPNs for access to MVD records in cases where no other connectivity is possible or the costs of such connectivity are prohibitive.
- Research indicates that IP Security (IPSec) will become the dominant standard for VPNs.

Background

In the pre-Internet days of computing, costly leased communication lines from the telcos (telephone companies) or dial-up modem-to-modem connections over analog telephone lines were the only viable options available to those who wanted to communicate with others in the outside world.

- Often, these communication links could only carry the traffic for a single network protocol (such as IBM's SNA and TTY traffic), necessitating additional lines for each new protocol.
- These links were point-to-point. A dedicated connection could only be used from Point A to Point B. If Point A needed to communicate with Point C, another line was mandatory. As complexity increased, networks grew among multiple external companies and expenses began to soar. Beside inter-company communications, businesses created branch offices, remote factories, and far-flung sales sites. These isolated facilities had their own communication needs
- Wide Area Network (WAN) development and support required additional dedicated links or satellite communications to attain the high availability that's required.
- As organizations began to encourage remote employee access to internal networks (LANs), huge banks of modems became prevalent -- requiring additional capital

investments and support costs that were already becoming unmanageable.

- Over time, the symptoms that companies experienced with difficult-to-manage networked connections began to include never-before-witnessed problems, such as…
- Unreasonably long lead times to install and test new communication links
- Finger pointing among users, telcos, and equipment providers as communication problems arose
- Skyrocketing support and management costs
- Increased complexity in all aspects of hardware, software, and dependence on multiple service providers
- Difficulties in scaling up as needs dictated

Once the Internet was deemed a viable alternative to dedicated and dial-up computer links, organizations began to hop on the bandwagon, hoping to drive down the costs of operation. Without effective security and reliability in place, however, any hopes of migrating to the Internet were quickly dashed. To serve these aspiring business users, new technologies entered the scene.

Approach

Employees in the ADOT TIR Department initiated evaluation and testing vpn technology early in the first phase of this project using equipment and software that ADOT already owned. The intent was for TIR to make a recommendation to ADOT for a system was deemed both reliable and secure. Two systems were tested:

1. Microsoft Windows 2000 VPN

2. Checkpoint VPN1

These products were tested in the laboratory using one Compaq Proliant server and 3 Compaq workstations, including one laptop computer. These were attached using 100MB Ethernet.

Problems with the Checkpoint firewall appeared early and with any ability to troubleshoot the interaction between the Checkpoint system and Windows NT, further efforts at testing were abandoned. The results of testing the Checkpoint VPN are summarized below in Table 3.1

Table 3.1: Checkpoint VPN Testing

Application	Pass/Fail	Reliability and comments
Telnet	Pass	Good
FTP	Pass	Good
MS Outlook (e-mail)	Fail	50% reliability - unknown causes
MS Networking (file access)	Fail	50 reliability - unknown causes

Concentrating on the Windows 2000 VPN solution, using Microsoft's implementation of PPTP, the team was able to successfully install and access the suite of applications that remote users of ADOT systems would normally access.

The results of the Windows 2000 VPN using 128-bit encryption are shown in Table 3.2.

Table 3.2: Results of the Windows 2000 VPN		
Application	**Pass/Fail**	**Reliability and comments**
Telnet	Pass	Good
FTP	Pass	Good
MS Outlook (e-mail)	Pass	Good
MS Networking (file access)	Pass	Good
SMS 1.2	Pass	Good
HEAT (OBDC)	Pass	Good
MS Terminal Server	Pass	Good
MS SQL Server	Pass	Good

Notes from the evaluation report indicate that all applications tested successfully without any connectivity or performance problems. Network bandwidth never exceeded 50% utilization.

Once the technology was proven sufficient for TIR requirements, the pilot test was expanded to other internal ADOT employees who used a variety of workstations, including MS Windows 2000, Microsoft NT Workstation, and Microsoft Windows 95/98. Connection types also varied. Users accessed the Internet using Digital Subscriber Line (DSL), Cable modems, traditional dial-up, and even 2-way wireless technology. A number of different ISPs were used by the testers as well, including:

- Bizillion
- USWest/Qwest
- COX@Home
- AOL
- Sprint broadband

The pilot ran from April 2000 through August 2000 when it was determined that the Windows 2000 VPN met the criteria for a TIR recommendation to ADOT to proceed with expanding the pilot to select MVD third-parties.

Findings

Due to ADOT's commitment to the Microsoft product line for both infrastructure (networks and OSs) and application programs (terminal server, Outlook, etc.), using VPNs other than Microsoft's was thought to lead to support and reliability problems. Marketplace research supports this theory. Since many of the protocols used within the Microsoft family of products are atypical of the protocols most often found on the Internet. The support that vendors other than Microsoft are providing on their VPN products often do not work well with Microsoft protocols, but this will not always be the case. As VPN technology matures and standards shake themselves out, in the future VPN products should become fungible. However in today's marketplace reality they're not quite there yet and organizations simply cannot wait.

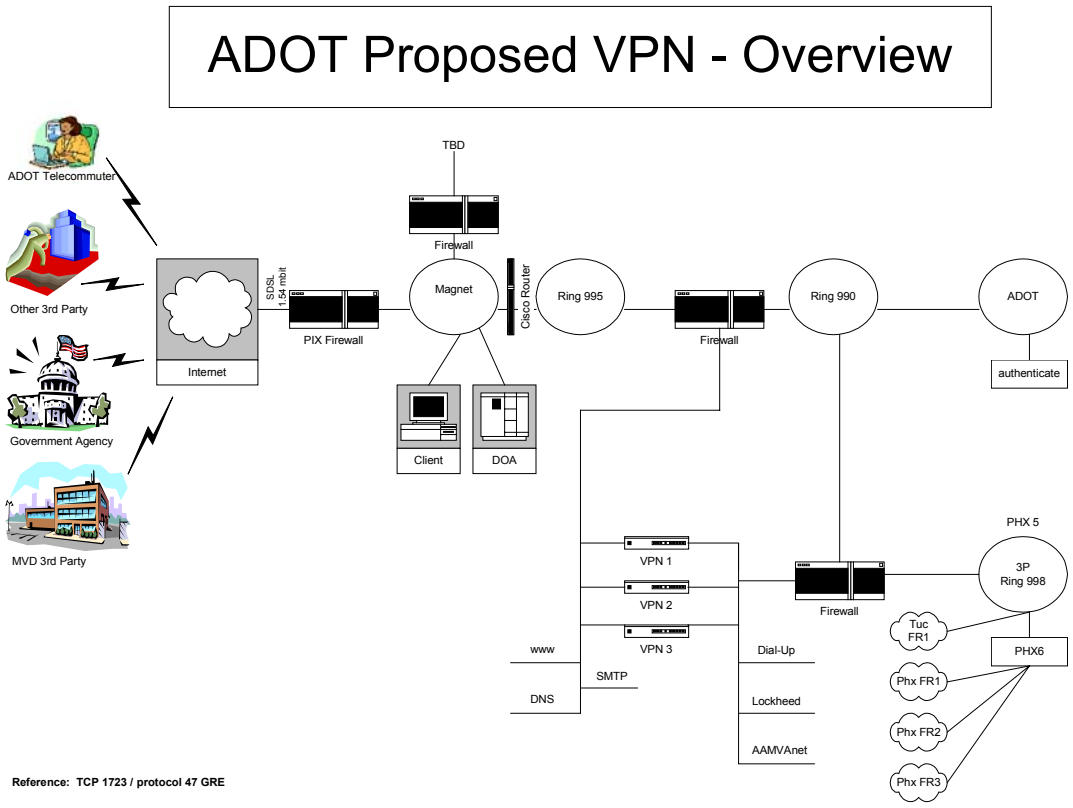
As a participant in the standards process, Microsoft pledges support on future products for whatever the industry standard calls for and has provided a migration path for users. Despite the criticisms of Microsoft's implementation of PPTP, what's important is that the system does operate as needed and still provides the sufficient layer of security needed to protect MVD records.

Research indicates that IP Security (IPSec) will become the dominant standard for VPNs. In today's environment however, implementing an IPSec VPN and expecting full interoperability and reliability is still too premature. For those organizations who operate their systems based only on the 'purist' protocols upon which the Internet was built, IPSec-based VPNs are likely to work well. On the other hand, those who use other types proprietary protocols (like Microsoft) are given two basic choices:

- Wait until the standards shake themselves out, then invest in the technology
- Tip-toe slowly into the technology by adopting 'what works today' with an eye to a point of arrival migration (wherever that may be).

TIR opted for the second choice.

In late-October 2000, a Project and Investment Justification (PIJ) was prepared to use the research dollars tied to capital investments to purchase the hardware and needed to offer load-balancing, fail-over, and improved reliability. The proposed network architecture is shown in Figure 3-1 below.



The full report *ADOT Uses for Virtual Private Networking Technology: Phase 1 – Pre-Pilot Test Report* by Mark Merkow (Arizona Department of Transportation, report number FHWA-AZ-01-502(1), published February 2001) is available from the Arizona Transportation Research Center, 206 S. 17 Ave., mail drop 075R, Phoenix, AZ 85007; phone 602-712-3138.